

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

FILED
 AUG 10 2022
 Mark C. McCartt, Clerk
 U.S. DISTRICT COURT

In the Matter of the Search of
*An Apple iPhone in red case specifically described in Attachment A,
 currently located at 8023 E. 63rd Place, Tulsa, Oklahoma*

Case No. 22-mj-503-CDL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

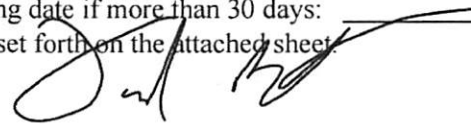
The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 1151, 1152, and 2241	Aggravated Sexual Abuse in Indian Country
18 U.S.C. § 2251	Production of Child Pornography
18 U.S.C. §§ 1151, 1152, and 2252	Possession of Child Pornography in Indian Country

The application is based on these facts:

See Affidavit of Daniel Berardicurti, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SA Daniel Berardicurti, FBI

Printed name and title

Sworn to ^{by telephone} before me and signed in my presence.

Date: August 10, 2022


Judge's signature

City and state: Tulsa, OK Tulsa, Oklahoma

Hon. Christine D. Little, U.S. Magistrate

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH
OF AN APPLE IPHONE IN RED
CASE SPECIFICALLY DESCRIBED
IN ATTACHMENT A, CURRENTLY
LOCATED AT 8023 E. 63rd PLACE,
TULSA, OKLAHOMA

Case No. _____

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Daniel Berardicurti, being first duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—one electronic device described in **Attachment A** (hereinafter the “Device”)—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in **Attachment B**.¹

2. I am a Special Agent with Federal Bureau of Investigation and have been since January 2019. I maintain a Juris Doctorate and an active membership in the Texas State Bar. Prior to being a Special Agent with the Federal Bureau of Investigation I was a police officer for approximately three years. During that time, I investigated numerous violent crimes as a first responder and drafted numerous

¹ This application is a follow-up to the search warrant authorized in 22-MJ-484-CDL. The authorization for this search is necessary because the Device was seized at a location outside the scope of the previously authorized warrant. *See infra* at ¶ 38.

search warrants. Currently I am assigned to conduct investigations pursuant to the Federal Bureau of Investigations' Safe Trails Task Force, which focuses on a myriad of crimes occurring on Indian reservations to include sexual assaults of minors and production of child pornography. I have received basic and on-the-job training in the investigation of cases involving sexual assaults of minors and production of child pornography.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this Affidavit are based on my personal observations, knowledge obtained from other law enforcement officials, reviews of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Since this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth every fact I or others have learned during the course of this investigation.

4. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that the following criminal law violations have occurred: 18 U.S.C. §§ 1151, 1152, and 2241 (Aggravated Sexual Abuse in Indian Country), 18 U.S.C. § 2251 (Production of Child Pornography), and 18 U.S.C. §§ 1151, 1152, and 2252 (Possession of Child Pornography in Indian Country). There is also probable cause to examine the Device described in

Attachment A for evidence, contraband, instrumentalities, and/or fruits of these crimes as further described in **Attachment B**.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The Device to be examined is an Apple iPhone in a red case seized from Justin Lee Smith's property at the David L. Moss Criminal Justice Center.

6. The Device is currently stored in the Tulsa Federal Bureau of Investigation Resident Agency located at 8023 E. 63rd Place, Tulsa, Oklahoma, within the Northern District of Oklahoma.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in **Attachment B**.

DEFINITIONS

8. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

- a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct

9. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

10. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

11. The term “computer,” as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

12. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

**CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO
PRODUCE, COLLECT, RECEIVE, OR DISTRIBUTE CHILD
PORNOGRAPHY**

13. Based on my previous experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

- a. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Likewise, individuals with intent to view and/or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by,

usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

- d. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- e. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- f. Individuals who coerce and entice minors may use alcohol and/or narcotics to lower the inhibitions of children they are attempting to seduce.

BACKGROUND ON DIGITAL MEDIA STORAGE DEVICES AND CHILD PORNOGRAPHY

14. The ability of a computer (including a smartphone) to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Given the storage capabilities, modern computers can retain many years' worth of a user's data, stored indefinitely. Even deleted data can often be forensically recovered. Other digital media storage devices (e.g., compact disks, digital video disks, thumb drives,

etc.) can also store tremendous amounts of digital information, including digital video and picture files.

15. I know smartphones (a type of “computer,” as broadly defined in 18 U.S.C. § 1030(e)(1)) like an iPhone can typically “sync” with a traditional desktop or laptop computer. The purpose of syncing a smartphone to a traditional computer is to back up data that is stored on the phone so that it is not permanently lost if the portable smartphone is lost or damaged. Also, smartphone users may move files off the smartphone and onto a computer to free up storage space on the smartphone. Similarly, computer (e.g., desktop computers, smartphones, etc.) users may move files off of one computer onto another computer or digital file storage devices such as a thumb drive, a DVD, or an external hard drive to free up space on the computer.

PROBABLE CAUSE

16. At all times relevant to this Affidavit, the sixteen-year-old victim, A.B., was and is a member by blood of the Choctaw Nation of Oklahoma (Citizen ID: XXXXXX50) according to a certificate of citizenship issued by the Choctaw Nation of Oklahoma. The suspect is Justin Lee Smith, a 45-year-old non-Indian male. During initial questioning, Smith told officers that he is a non-Indian, and a records check by police confirmed this.

17. The incidents referred to in this Affidavit occurred at a residence on East 25th Street in Tulsa, Tulsa County, State of Oklahoma, Northern District of Oklahoma, and within the Cherokee Nation Indian Reservation, which is Indian country as defined in 18 U.S.C. § 1151.

18. As part of this investigation, I reviewed law enforcement reports, victim statements, officer worn body camera footage, and the forensic interview of A.B., who detailed her sexual abuse at the hands of Smith during the forensic interview. The investigation thus far has yielded the following information.

19. A.B. was at Smith's East 25th Street house during the evening of August 7, 2021. Smith is a neighbor and friend of A.B.'s mother, and A.B. was at the house to make some extra money helping with chores. A.B. said that both families were going to go to the racetrack later that evening.

20. A.B. said that Smith's five-year-old grandson, and eleven-year-old female cousin, were also visiting Smith that day. A.B. said this was a common occurrence.

21. A.B. stated that at some point Smith shut and locked his bedroom door, isolating the two of them alone inside. A.B. said Smith started rubbing a ball on her upper back and it felt "weird".

22. A.B. said that Smith forced her onto the bed. A.B. said Smith pushed her onto her back by pushing her shoulders with his hands. Smith pulled her pants and boxers off and "shimmied" his pants partly down his thigh. A.B. said she struggled and struck Smith in attempts to stop him. A.B. said she repeatedly said "no" to Smith. Smith forced his penis inside of A.B.'s vagina.

23. A.B. said after Smith finished assaulting her, he told her not to tell anyone or "bad things happen." She took this as a threat and was scared to even leave his house immediately. She said she stayed there until he went back into his

bedroom, and she felt she could leave.

24. A.B. ran home crying and shaking. She told her mother, C.B., what happened, and the Tulsa Police Department was called out to investigate. Prior to their arrival, C.B. attempted to confront Smith about the incident. He reportedly told her that he recorded it.

25. Tulsa Police officers made contact with Smith, who stated that A.B. often came to his residence. Smith told officers that he was “back there fooling around” with A.B. Smith told officers he rubbed on A.B.’s “butt” and recorded it. Smith told officers that it was just some rubbing “and shit like that”. Smith reiterated to officers that he recorded it. Smith told officers that the recording is on his telephone and produced for them his white iPhone. Smith told officers the incident happened “just a little while ago”. Smith showed officers some images of A.B. on his iPhone and stated he deleted “some shit in a panic.”

26. Smith told officers “fucking lust got to me”. Smith also told officers “we got frisky . . . consider it all the way to third base . . . I fingered her, too.”

27. Tulsa Police Officer Tsaras read Smith his *Miranda* rights. Smith stated he understood. Smith continued to talk and show his iPhone to officers. He showed Officer Morris a video that Smith described as “just the rubbing—never penetration”. Smith told officers he had a few videos on his iPhone but he deleted them all. Smith stated he rubbed his penis on A.B. While not visible on the officer’s body worn camera, Smith described one picture as showing A.B. in a “doggystyle” sex position and opined that he was not holding her down.

28. Smith told officers everything that occurred was consensual, but he apologized to A.B.

29. Officers collected Smith's iPhone as evidence and turned it into the Tulsa Police Property room as evidence on Property Receipt BS7046. The seized device was placed into Airplane mode to avoid remote deleting of evidence. The Apple iPhone is white and connected to the phone number of 539-222-9345.

30. On May 31, 2022, United States Magistrate Judge Susan B. Huntsman signed a search warrant for the search of Smith's iPhone. The FBI Computer Analysis Response Team subsequently extracted data from the phone.

31. Between July 7, 2022, and July 11, 2022, I reviewed the extraction. I observed several images and videos containing the sexually explicit material described by A.B. and Smith, including a video that appears to be sexual intercourse between the two on August 7th. I further located an image, dated July 11, 2021, of an unknown blonde individual that appears to be a minor.

32. The minor is facing away from the camera and laying on the body of an adult male. Both the adult male and the minor appear to be nude. While I am unable to ascertain if the minor is a male or female, I know from review of the evidence in this case that Smith often cares for his young son who has blonde hair.

33. This and several other aforementioned images have GPS coordinates associated to them. A Google search of the GPS coordinates show that the images were taken in the area of 12906 E 25th Street, Tulsa, Oklahoma (Smith's home at the time of the assault of A.B.).

34. As a result of the May 31st search warrant, I also located other evidence. There were other photographs taken of A.B. prior to August 7, 2021, that appear to have been taken candidly. I located internet searches of A.B. in July of 2021. I also located internet searches regarding the Oklahoma age of consent laws dated August 7, 2021.

35. On July 13, 2022, I utilized open-source reporting to locate Smith's current residence and learned he lives at 2328 W. Galveston Street, Broken Arrow, Oklahoma 74012. On July 14th, I physically surveyed the home. I saw a white Toyota Tacoma bearing Oklahoma license plate LHA532 back out of the garage and exit the driveway. As a law enforcement officer, I have access to the National Crime Information Center, which is a computerized index of criminal justice information. I utilized NCIC to search for that license plate and discovered Justin Lee Smith is the owner of the vehicle.

36. On July 29, 2022, United States Magistrate Judge Christine D. Little authorized a search warrant for 2328 W. Galveston Street, in Case No. 22-MJ-484-CDL.

37. On August 1, 2022, Smith was indicted for one count of violating 18 U.S.C. § 2251(a) and 2251(e) (Production of Child Pornography) and one count of violating 18 U.S.C. § 2252(a)(4)(B) and 2252(b)(2) (Possession of Child Pornography).

38. On August 5, 2022, Smith was arrested by officers from the Tulsa Police Department during a traffic stop away from his residence. Officers seized the

Device—an Apple iPhone, inside of a red case—from Smith’s possession. The Device was placed in airplane mode. The iPhone was transported with Smith to the David L. Moss Criminal Justice Center where it was logged into Smith’s property. Because of the location where the Device was seized, it was not covered by the scope of the search warrant authorized in 22-MJ-484-CDL.

39. After Smith’s arrest, the search warrant for 2328 W. Galveston Street was executed by members of the FBI. During the search, multiple personal electronic devices were located and seized, including: a Cyber Power PC desktop computer, a black iPhone, an LG cellular phone, and a white Samsung cellular phone. Agents also located a life-size, anatomically correct, naked child sex doll in Smith’s closet. The doll was similar in nature to the image referenced in paragraphs 31 and 32.

40. On August 8, 2022, Special Agent Tiffany Harrison and I went to the David L. Moss Criminal Justice Center to transport Smith. During the transport process, I seized the Device. Staff Operation Specialist Tylor Reed preserved Justin Lee Smith’s Apple account with correspondence to Apple.

41. I am specifically requesting all records and evidence located on the Device because, based on my training and experience, I know that cellular phones and other recording devices can be backed up on computers. *See supra* p. 6-7. I also know that an iPhone will automatically “back-up” photographs and store them on the “iCloud.” This automatic “back-up” is the standard setting for iPhones. Users can utilize the “iCloud,” which securely stores photos, files, and other data, and

syncs the information across all of a users' devices. I know that iCloud accounts can be accessed using computers, meaning that Smith could access information viewable on the phone currently in police custody by way of the cloud using an electronic device currently in his possession.

42. Further, I am requesting all items described in **Attachment B** without date and time restrictions. This is for multiple reasons. First, the initial review of Smith's iPhone, as described above, indicates that he was conducting internet searches for A.B. prior to his sexual intercourse with her. A review of the entirety of digital evidence recovered from his home can demonstrate how far in advance Smith was planning to engage in sexual contact with A.B. or other minors. Additionally, a review of all recovered evidence will assist in identifying the unknown blonde individual, believed to be a minor. Viewing all of the requested data without date and time restrictions will allow me to identify this, and other, potential victims.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

43. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

44. There is probable cause to believe that things once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium,

deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

45. As further described in **Attachment B**, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from

a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to produce, receive, and possess child pornography, the individual’s electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to

commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

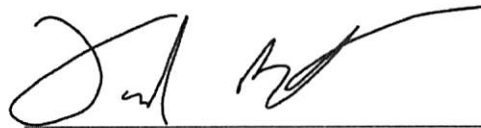
46. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection to determine whether it is evidence described by the warrant.

47. This warrant seeks only permission to examine devices already in law enforcement's possession, and therefore the execution of said warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

48. I submit that this Affidavit supports probable cause for a search warrant authorizing the examination of the Device described in **Attachment A** to seek the items described in **Attachment B**.

Respectfully Submitted,

A handwritten signature in black ink, appearing to read 'Daniel Berardicurti', written over a horizontal line.

Special Agent Daniel Berardicurti
Federal Bureau of Investigation

SUBSCRIBED TO AND SWORN TO by phone on this 10th day of August, 2022.

A handwritten signature in blue ink, appearing to read 'Christine D. Little', written over a horizontal line.

Honorable Christine D. Little
United States Magistrate Judge

ATTACHMENT A

Property to be searched

The property to be searched, an Apple iPhone in a red case (hereinafter the “Device”) is currently located at the Tulsa Federal Bureau of Investigation Resident Agency located at 8023 E. 63rd Place, Tulsa, Oklahoma, within the Northern District of Oklahoma. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in **Attachment B**.

ATTACHMENT B

Property to be seized

All records on the Device described in **Attachment A** that relate to violations of 18 U.S.C. §§ 2241, 2251, 2252, including, but not limited to the following records:

A. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found, including, but not limited to:

- i. Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG) of child pornography; files relating to the distribution, receipt, or possession of child pornography, or information pertaining to an interest in child pornography;
- ii. Files in any form containing the visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and

iii. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors.

B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

iii. Any and all electronic and/or digital records and/or documents including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in 18 U.S.C. § 2256; or relating to the sexual exploitation of minors;

- iv. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums;
- v. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;
- vi. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and
- vii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software.

C. Records or other items which evidence ownership, use, or control of the Device described in Attachment A.

D. Any and all correspondence, in whatever form, with A.B. and C.B.

E. Any and all information, correspondence (including emails), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educating, enticing, coercing, or persuading a minor to engage in sexual acts.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.